PCT/KR 2004/001911
RO/KR 29.07.2004

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0095373
Application Number

출 원 년 월 일 : 2003년 12월 23일
Date of Application DEC 23, 2003

출 원 인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Ins

2004 년 06 월 23 일

특 허 청
COMMISSIONER

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0027
【제출일자】	2003.12.23
【국제특허분류】	H04L
【발명의 명칭】	디지털 로직을 이용한 난수 발생 장치 및 방법
【발명의 영문명칭】	Apparatus and method for generating random number using digital logic
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	2001-038378-6
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2001-038396-8
【발명자】	
【성명의 국문표기】	전용성
【성명의 영문표기】	JEON,Yong Sung
【주민등록번호】	680518-1674516
【우편번호】	302-792
【주소】	대전광역시 서구 월평동 302번지 황실타운아파트 112동 1005호
【국적】	KR
【발명자】	
【성명의 국문표기】	박지만
【성명의 영문표기】	PARK,Ji Man
【주민등록번호】	670928-1386421

【우편번호】 305-752
【주소】 대전광역시 유성구 송강동 청솔아파트 310-1208
【국적】 KR
【발명자】
【성명의 국문표기】 박영수
【성명의 영문표기】 PARK,Young Soo
【주민등록번호】 620807-1149123
【우편번호】 302-766
【주소】 대전광역시 서구 탄방동 산호아파트 101동 907호
【국적】 KR
【발명자】
【성명의 국문표기】 전성익
【성명의 영문표기】 JUN,Sung Ik
【주민등록번호】 620428-1925812
【우편번호】 305-755
【주소】 대전광역시 유성구 어은동 한빛아파트 107동 704호
【국적】 KR
【발명자】
【성명의 국문표기】 정교일
【성명의 영문표기】 CHUNG,Kyo Il
【주민등록번호】 571103-1006113
【우편번호】 305-707
【주소】 대전광역시 유성구 신성동 한울아파트 107동 1102호
【국적】 KR
【심사청구】 청구
【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
이영필 (인) 대리인
이해영 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	2	면	2,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	12	항	493,000 원

【합계】 524,000 원
【감면사유】 정부출연연구기관
【감면후 수수료】 262,000 원
【기술이전】
【기술양도】 희망
【실시권 허여】 희망
【기술지도】 희망
【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

디지털 로직을 이용한 난수 발생 장치 및 방법이 개시되어 있다. 난수 발생 장치는, 내부에 저장된 비트 값들을 순차적으로 이동시키는 쉬프트 레지스터, 상기 쉬프트 레지스터에 저장된 비트 값들을 소정 논리 연산하여 생성한 궤환신호를 생성하는 궤환회로, 쉬프트 레지스터로 입력되는 외부 신호를 생성하는 외부신호 생성회로, 및 궤환신호 및 외부신호를 소정 논리연산하여 쉬프트 레지스터로 출력하는 입력 논리회로를 포함하고, 난수 발생 방법은, 쉬프트 레지스터 내부에 저장된 비트 값들을 순차적으로 이동시키는 단계, 쉬프트 레지스터에 저장된 비트 값들을 소정 논리연산하여 궤환신호를 생성하는 단계, 쉬프트 레지스터로 입력되는 외부 신호를 생성하는 단계, 및 궤환신호 및 외부신호를 소정 논리연산하여 쉬프트 레지스터로 출력하는 단계를 포함한다.

【대표도】

도 1

【명세서】

【발명의 명칭】

디지털 로직을 이용한 난수 발생 장치 및 방법{Apparatus and method for generating random number using digital logic}

【도면의 간단한 설명】

도 1은 본 발명에 따른 디지털 로직을 이용한 난수 발생 장치의 일 실시예의 개략적인 블록도이다.

도 2는 도 1의 쉬프트 레지스터 및 궤환회로를 4비트 선형 궤환 쉬프트 레지스터로 구성한 개략적인 블록도이다.

도 3은 도 2의 구성에 고정값 방지회로를 추가한 구성의 개략적인 블록도이다.

도 4는 도 1의 랜덤신호 발생회로를 독립적인 발생원을 가지는 두개의 클럭을 이용하도록 구성한 일 실시예의 개략적인 블록도이다.

도 5는 도 1의 랜덤신호 발생회로를 독립적인 발생원을 가지는 두개의 클럭의 라이징 및 폴링 에지를 이용하도록 구성한 다른 실시예의 개략적인 블록도이다.

도 6은 본 발명에 따른 디지털 로직을 이용한 난수 발생 방법의 일 실시예를 수행하는 흐름도이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<7> 본 발명은 난수 발생 장치 및 난수 발생 방법에 관한 것으로서, 더욱 상세하게는 디지털 로직을 이용한 난수 발생 장치 및 난수 발생 방법에 관한 것이다.

<8> 난수 발생 장치는 암호연산을 위한 키의 생성 등의 여러 가지 목적에 사용되며 이와 같은 암호연산의 안전을 보장하기 위해서는 난수 발생 장치의 성능이 무엇보다 중요하다고 할 수 있다.

<9> 난수가 되기 위해서는 통계적으로 모든 값이 골고루 발생할 수 있는 복잡도를 유지하여야 하며, 난수의 값을 예측할 수 없는 랜덤성을 가지고 있어야 한다. 난수를 발생시키는 기존의 방법으로는 물리현상에서 발생하는 노이즈 성분을 이용한 물리적 난수 생성 방법과 수학적으로 정의된 일정한 수열을 발생시키는 의사 난수생성 방법으로 크게 나눌 수 있다.

<10> 물리적 난수를 만들기 위한 기존 방법은 기존에는 열잡음이나 온도, 전원 공급기의 전력 변화 등과 같은 물리현상을 이용하는 것이다. 물리적 현상을 이용함으로써 근본적으로 암호학적으로 안전한 난수라고 볼 수 있으나 난수를 얻기 위해서는 물리 현상의 신호가 매우 작기 때문에 이를 증폭하기 위한 증폭 회로 및 기타 부가적인 아날로그 회로가 필수적이다.

<11> 또한, 아날로그 회로는 랜덤성을 가지는 신호를 생성할 뿐이며, 통계적으로 균형 잡히고 충분한 복잡도를 가지는 디지털 난수 값을 얻기 위해서는 아날로그 신호를 샘플링하고 이를 다시 모으는 콜렉터 로직이 필요하다.

<12> 기존의 콜렉트 로직은 난수 스트림을 생성하기 위해 많은 시간이 필요로 하여 높은 성능의 암호 처리에는 부적합할 수 있다. 또한 아날로그 회로를 이용한 난수 발생장치는 칩 공정에 맞게

구현이 어려울 뿐만 아니라 난수 발생에 필요한 전압원이 공격자에 의해 제어되기 쉬운 단점을 가지므로 충분한 성능을 얻기 위해서는 많은 실험 및 노력을 필요로 한다.

<13> 이와 같은 물리적 현상을 이용한 난수 외의 또 다른 난수 발생 방법인 의사난수는 디지털 로직만을 이용하므로 구현이 용이하여 많은 시스템에서 사용되고 있다. 종래의 의사 난수 발생 방법은 선형 합동 발생기 알고리즘(Linear Congruential Generator Algorithm) 또는 선형 피드백 쉬프트 레지스터(LFSR : Linear Feedback Shift Register) 등을 이용하고 있다.

<14> 그러나, 이들 의사 난수 발생 방법은 수학적으로 정의된 함수로부터 얻어진 수열을 순차적으로 출력함으로써, 생성될 난수 값이 미리 정의되어 있고, 정의된 수열이 순차적으로 출력되다가 일정 시간이 지난 후, 동일한 순서를 다시 반복하므로 충분히 예측할 수 있는 난수를 발생시키게 된다. 예를 들어, 선형 합동 발생기 알고리즘의 경우 동일한 값을 입력하면 동일한 출력을 발생하게 되고, 선형피드백 쉬프트 레지스터 경우도 동일한 초기 입력값 즉, 시드(seed)를 입력한 후 동일한 시간이 지난 후의 출력 값은 항상 동일하다.

<15> 결국 의사난수는 통계적으로 모든 값이 골고루 발생할 수 있는 복잡도를 보장할 수는 있지만 특정한 초기 입력값에 대한 동일한 시간의 출력은 예측 가능한 값을 가지므로 랜덤성을 만족시키지 못하고 있다. 따라서 의사난수를 이용하는 시스템은 초기 입력값인 시드를 랜덤하게 얻기 위한 별도의 노력이 필요하게 된다.

【발명이 이루고자 하는 기술적 과제】

<16> 본 발명이 이루고자 하는 기술적 과제는 디지털 로직만을 이용하여 구현이 용이하면서도, 아날로그 회로를 이용한 물리적 난수 발생 장치가 가지는 랜덤성을 유지할 수 있는 디지털 난수 발생 장치 및 난수 발생 방법을 제공하는 것이다.

【발명의 구성 및 작용】

<17> 상기의 문제점을 해결하기 위해, 본 발명은 디지털 로직만을 이용하여 아날로그 회로를 이용한 물리적 난수발생장치가 가지는 랜덤성을 유지하면서 구현이 용이한 난수 발생 장치 및 난수 발생 방법을 제공한다. 본 발명은 선형 피드백 쉬프트 레지스터의 피드백 부에 랜덤성을 가지는 신호를 합하여 입력하는 경우 선형피드백 쉬프트레지스터(LFSR)에서 생성되는 값들이 랜덤성을 가지게 되는 점과, 클럭 값이 변화하는 시점이 매 클럭마다 일정치 않은 지트 성분을 가지고 있는 점을 이용하여 디지털 회로만으로 완전 난수를 발생시키는 구성을 제공한다.

<18> 본 발명의 제1관점에 따른 디지털 로직을 이용한 난수 발생 장치는, 내부에 저장된 비트 값들을 순차적으로 이동시키는 쉬프트 레지스터, 상기 쉬프트 레지스터에 저장된 비트 값들을 소정 논리연산하여 생성한 궤환신호를 생성하는 궤환회로, 상기 쉬프트 레지스터로 입력되는 외부신호를 생성하는 외부신호 생성회로, 및 상기 궤환신호 및 외부신호를 소정 논리연산하여 상기 쉬프트 레지스터로 출력하는 입력 논리회로를 포함하는 것을 특징으로 한다.

<19> 또한, 바람직하게는 상기 쉬프트 레지스터의 비트 값 및 외부 신호의 논리값이 모두 동일한 경우, 상기 입력 논리회로의 출력값이 상기 쉬프트 레지스터의 비트 값과 다른 값이 되도록 하는 값을 상기 입력 논리회로로 출력하는 고정값 방지회로를 더 포함하는 것을 특징으로 한다.

<20> 또한, 바람직하게는 상기 고정값 방지회로의 출력은 논리값 하이(high)인 것을 특징으로 한다.

<21> 또한, 바람직하게는 상기 외부 신호 생성회로는 랜덤신호를 생성하는 것을 특징으로 한다.

<22> 또한, 바람직하게는 상기 랜덤신호는 발생원이 다른 신호를 샘플링함으로써 생성되는 것을 특징으로 한다.

<23> 또한, 바람직하게는 상기 샘플링은 신호의 라이징 에지 및 폴링 에지에서 모두 수행되는 것을 특징으로 한다.

<24> 본 발명의 제2관점에 따른 디지털 로직을 이용한 난수 발생 방법은, 쉬프트 레지스터 내부에 저장된 비트 값들을 순차적으로 이동시키는 단계, 상기 쉬프트 레지스터에 저장된 비트 값들을 소정 논리연산하여 궤환신호를 생성하는 단계, 상기 쉬프트 레지스터로 입력되는 외부 신호를 생성하는 단계, 및 상기 궤환신호 및 외부신호를 소정 논리연산하여 상기 쉬프트 레지스터로 출력하는 단계를 포함하는 것을 특징으로 한다.

<25> 또한, 바람직하게는 상기 쉬프트 레지스터의 비트 값 및 외부 신호의 논리값이 모두 동일한 경우, 상기 쉬프트 레지스터로의 출력값이 상기 쉬프트 레지스터의 비트 값과 다른 값이 되도록 하는 고정 방지값을 더 논리연산하는 것을 특징으로 한다.

<26> 또한, 바람직하게는 상기 고정 방지값은 논리값 하이인 것을 특징으로 한다.

<27> 또한, 바람직하게는 상기 외부 신호는 랜덤신호인 것을 특징으로 한다.

<28> 또한, 바람직하게는 상기 랜덤신호는 발생원이 다른 신호를 샘플링함으로써 생성되는 것을 특징으로 한다.

<29> 또한, 바람직하게는 상기 샘플링은 신호의 라이징 에지 및 폴링 에지에서 모두 수행되는 것을 특징으로 한다.

<30> 본 발명에 의해 난수를 발생함에 있어서, 디지털 로직만을 이용하여 구현이 용이하면서도, 아날로그 회로를 이용한 물리적 난수 발생 장치가 가지는 랜덤성을 유지할 수 있게 된다. 또한,

의사 난수 발생 장치인 선형피드백 쉬프트 레지스터가 가지는 특성을 이용함으로써 통계적으로 모든 값이 골고루 발생할 수 있는 복잡도를 만족시키게 된다.

<31> 본 특허에서 제시하는 발명 가운데 대표적인 개요를 설명하면 다음과 같다. 기존의 의사 난수 발생 방법에 사용되는 선형 궤환 쉬프트 레지스터는 수학적으로 정의된 함수로부터 얻어진 궤환 회로를 이용하여, 이 궤환회로의 출력을 쉬프트 레지스터로 입력시킴으로써 매 클럭마다 다른 수열을 발생시키게 되지만, 앞서 설명한 바와 같이 발생하는 수열의 순서가 고정되는 단점을 가지고 있다. 이와 같은 단점을 극복하기 위해 본 발명은 쉬프트 레지스터의 입력으로 기존의 궤환회로의 출력 외에 또 다른 외부신호를 함께 합(+)함으로써 다른 특성을 가지는 난수발생장치를 제공한다.

<32> 이 외부신호가 0 또는 1의 랜덤신호를 계속하여 발생하게 되면 전혀 다른 특성의 선형 궤환 쉬프트 레지스터가 된다. 외부신호가 0인 경우는 기존의 선형궤환 쉬프트 레지스터와 동일한 순서의 수열이 생성되지만, 반면 이 외부 신호가 1인 경우는 쉬프트 레지스터의 수열 순서가 0인 경우의 반대 순서가 되는 것이 아니라, 또 다른 순서를 가지게 된다. 또한 외부신호가 1인 경우도 레지스터에서 생성되는 수열 값의 발생 분포가 동일하여 0인 경우와 같은 복잡도를 유지하게 된다. 따라서 외부신호가 랜덤 값을 발생하면 선형궤환 쉬프트 레지스터에서 생성되는 수열은 예측 불가능한 난수가 된다.

<33> 기존의 난수 발생 장치가 아날로그 회로를 이용하여 생성된 신호의 랜덤성을 지속적으로 누적시키지 못하고 최근에 생성된 랜덤신호만을 이용하여 난수를 발생시키고 있는 것과는 달리, 본 발명이 제시하는 난수발생기의 우수한 특성은 기본적으로 쉬프트 레지스터에 의해 수열이 계속해서 다른 값으로 바뀌고 있는 가운데 랜덤신호 값에 의해 쉬프트 레지스터의 값의 변화 패

턴이 달라지기 때문에, 랜덤신호의 변화가 계속해서 누적되어 소프트웨어에서 난수를 필요로 하는 시점이 되면 쉬프트 레지스터에는 예측 불가능한 완전난수가 생성된다.

<34> 따라서 본 발명에서 제공하는 선형궤환 쉬프트 레지스터를 이용하면 쉬프트 레지스터에 입력되는 외부신호는 난수를 필요로 하는 시점 이전의 어느 시점이라도 랜덤한 특성을 가지면 쉬프트 레지스터는 예측 불가능한 수열을 생성하게 되므로, 랜덤한 외부신호를 얻기 위해 별도의 아날로그 회로를 이용하지 않고 디지털 로직을 이용하여 간단히 구현될 수 있다.

<35> 본 발명에서 제공하는 선형궤환 쉬프트 레지스터에 입력되는 랜덤한 외부신호를 만들기 위해 사용하는 방법은 클럭 신호의 지트를 이용하는 것으로 두 개의 독립적인 소스에서 생성된 클럭을 이용하여 하나의 클럭이 또 다른 클럭의 값을 샘플링하는 것이다. 이와 같은 방법이 지트의 발생시간이 짧은 관계로 기존의 아날로그 회로를 이용한 랜덤신호 생성 방법에 비해서는 랜덤성이 떨어지는 신호를 발생시키지만, 난수를 필요로 하는 시간에는 충분히 많은 지트의 샘플링이 이루어진 이후이고, 매번 지트를 샘플링할 때마다 선형궤환 쉬프트레지스터의 값은 예측할 수 없는 값으로 바뀌게 되므로 지트의 랜덤 성분에 의해 선형궤환 쉬프트레지스터는 예측할 수 없는 난수를 생성하게 된다.

<36> 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 설명한다 발명의 이해를 돕기 위해 도면 전체에서 동일한 장치에 대해서는 동일한 부호를 사용한다..

<37> 도 1은 본 발명에 따른 디지털 로직을 이용한 난수 발생 장치의 일 실시예의 개략적인 블록도이다. 본 발명이 제시하는 난수 발생 장치는 크게 네 개의 블록으로 나뉘어 지는데 각 블록의 구성 및 동작에 대해 설명한다.

<38> 도 1의 난수 발생 장치는 쉬프트레지스터(100), 궤환회로(200), 고정값 방지회로(300), 랜덤신호 생성회로(400) 및 입력 논리회로(500)로 구성된다.

<39> 쉬프트 레지스터(100)는 내부에 저장된 비트 값들을 순차적으로 이동시키고, 궤환회로(200)는 쉬프트 레지스터(100)에 저장된 비트 값들을 소정 논리연산하여 생성한 궤환신호를 생성한다. 여기서 쉬프트 레지스터(100)와 궤환회로(200)는 종래의 선형궤환 쉬프트레지스터의 구성 방식을 따르게 되지만, 새로운 형태의 쉬프트 레지스터의 입력신호를 생성하는 방법, 고정값 방지회로(300), 랜덤신호 생성회로(400) 및 궤환회로(200), 고정값 방지회로(300) 및 랜덤신호 생성회로(400)의 출력을 합하여 쉬프트 레지스터(100)에 입력하기 위한 입력 논리회로(500)를 추가함으로써 전혀 다른 동작 특성을 가지는 난수발생 장치를 만들 수 있다.

<40> 본 발명의 난수발생장치의 동작 특성을 설명하기 위하여 하나의 실시예를 들어 설명하면 다음과 같다. 도 2는 새로운 구성 형태를 가지는 4비트 선형궤환 쉬프트레지스터를 나타내고 있다. 쉬프트 레지스터(100) 및 궤환회로(200)의 구성은 기존의 선형궤환 쉬프트레지스터의 방식을 따르게 되는데, 궤환회로(200)의 구성은 미리 정의된 원시 다항식에 의한 연산을 행하기 위한 것으로, 원시다항식은 $p(x) = x^4 + x^3+1$을 따른다. 도 2의 선형궤환 쉬프트레지스터가 기존의 것과 다른 부분은 쉬프트 레지스터(100)의 입력 신호가 궤환회로(200)의 출력 신호와 추가적인 외부신호를 합한 신호로 정해진 다는 것이다.

<41> 랜덤신호 생성회로(400)는 쉬프트 레지스터(100)로 입력되는 외부신호를 생성하는데 본 실시예에서는 외부신호는 랜덤신호이다. 외부신호가 계속해서 0인 경우는 궤환회로(200)의 출력만이 쉬프트 레지스터(100)의 입력으로 인가 되는 것과 같으므로 기존의 선형 궤환 쉬프트레지스터와 동일하게 된다. 이 경우, 쉬프트 레지스터(100)의 초기 시드(Seed)값이 1010 인 상태로 클럭에 따른 레지스터(110-140)의 변화 값을 나타내면 1010 , 1101 , 0110 ,

0011 , 1001 , 0100 , 0010 , 0001 , 1000 , 1100 , 1110 , 1111 , 0111 , 1011 , 0101 , 1010 의 순서가 된다.

<42> 반면, 외부신호가 계속해서 1인 경우는 쉬프트 레지스터(100)의 입력값은 궤환회로(200)의 출력값과 외부신호 값 1을 합한 값으로 결정된다. 이 경우, 쉬프트 레지스터(100)의 초기 시드(Seed)값이 1010 인 상태로 클럭에 따른 레지스터(110-140)의 변화 값을 나타내면 1010 , 0101 , 0010 , 1001 , 1100 , 0110 , 1011 , 1101 , 1110 , 0111 , 0011 , 0001 , 0000 , 1000 , 0100 , 1010 의 순서가 된다. 앞서 설명한 외부신호가 계속해서 0인 경우와 수열의 순서를 비교 해보면, 반대의 수열 순서가 되는 것이 아니라 또 다른 순서를 나타내게 되고, $2^4-1=15$개의 수열 값이 나오게 되므로 수열의 복잡도는 동일하다.

<43> 따라서 외부신호를 0과 1을 예측할 수 없는 랜덤신호를 연속적으로 생성하여 궤환회로(200)와 합하여 쉬프트 레지스터(100)로 입력하게 되면 쉬프트 레지스터의 값은 예측이 불가능한 값이 생성된다. 또한 외부신호가 랜덤한 값을 가지다가 어느 시간 이후에는 특정 값 또는 일정한 패턴을 가지는 경우이거나, 또는 랜덤 값을 가지는 신호와 특정 패턴 값을 가지는 신호가 주기적으로 반복되는 경우에도 랜덤 값이 입력되는 동안 쉬프트 레지스터는 이미 예측할 수 없는 값이 되어 있으므로 이후의 입력이 비록 특정 값 또는 특정 패턴이 되더라도 최종 쉬프트 레지스터의 값도 역시 예측이 불가능한 값이 된다. 이와 같은 특성은 기존의 난수 발생 장치에서는 찾아 볼 수 없는 특성으로서, 기존의 난수발생장치에서는 랜덤신호가 생성되다가 일정 시간이 지난 후, 특정 패턴의 신호가 생성되면 최종 난수 값도 특정 패턴의 값이 된다.

<44> 도 3은 도 2의 새로운 구성 형태를 가지는 4비트 선형 궤환 쉬프트레지스터에서 쉬프트 레지스터(100)의 수열이 매 클럭마다 바뀌지 않는 경우가 발생하는 것을 방지하는 고정값 방지회로

(300)를 추가한 것이다. 기존의 선형궤환 쉬프트레지스터는 궤환회로(200)의 출력만이 쉬프트 레지스터의 입력으로 인가되므로 시드 값이 모두 0이 아니라면 어떠한 경우에도 레지스터 (110-140)의 값이 모두 0이 되는 경우는 발생하지 않게 되며, 항상 매 클럭마다 정해진 패턴의 다른 값으로 바뀌게 된다.

<45> 그러나 본 발명이 제시하는 선형궤환 쉬프트레지스터는 궤환회로(200)의 출력과 추가적인 외부입력을 합하게 되므로 외부신호가 1인 경우에는 위에서 나열한 수열에서 알 수 있듯이 레지스터의 값이 모두 0이 되는 경우가 발생하게 된다. 만약 랜덤한 외부신호에 의해 레지스터 (110-140)의 값이 모두 0이 되는 순간 외부 입력값이 0으로 계속해서 고정되면 쉬프트 레지스터(100)는 클럭에 따라 값이 바뀌지 않고 계속해서 모든 값이 0으로 고정되게 된다. 마찬가지로 랜덤한 외부신호에 의해 레지스터(110-140)의 모든 값이 1이 되는 순간 외부 입력값이 1로 계속해서 고정되면 쉬프트 레지스터(100)는 클럭에 따라 값이 바뀌지 않고 계속해서 모든 값이 1로 고정되게 된다. 이와 같이 특정한 상황에서 쉬프트 레지스터(100)의 값이 고정되는 것을 방지하기 위한 수단으로 고정값 방지회로(300)가 필요하다.

<46> 이를 위해, 도 3에서는 레지스터(110-140)의 값 및 랜덤신호를 반전한 후 논리곱(또는 논리합한 후 반전)하는 회로(310)와, 레지스터(110-140)의 값 및 랜덤신호를 논리곱하는 회로(320)로부터 얻어지는 두 개의 출력을 논리합 회로(330)에서 논리 합(330)한 후, 이 논리합 회로(330)의 출력값과 랜덤신호의 값 및 궤환회로(200)의 출력값을 입력 논리 회로(500)에서 합하여 쉬프트 레지스터(100)에 입력함으로써 쉬프트 레지스터의 값이 고정되는 것을 방지하는 수단을 제공한다.

<47> 레지스터(110-140)의 값이 0000 이고 랜덤신호도 0이 되는 경우에, 고정값 방지회로(300)를 추가하지 않으면 궤환회로(200)의 출력값이 0이므로 이 궤환회로의 출출력값과덤 신호를 합

한 쉬프트 레지스터(100)의 입력값도 0이 되어 쉬프트 레지스터의 값은 계속해서 0000 을 유지하게 된다. 반면, 고정값 방지회로(300)를 추가하게 되면 레지스터(110-140)의 값 및 랜덤신호를 반전한 후 논리 곱(310)하는 출력은 1이 되므로, 논리합 회로(330)의 출력인 고정값 방지회로(300)의 출력도 1이 되어, 고정값 방지회로(300)의 출력 값, 랜덤신호, 그리고 궤환회로(200)의 출력값을 합한 회로(500)의 출력인 쉬프트 레지스터(100)의 입력값은 1이 된다. 결국 클럭에 의해 생성되는 쉬프트 레지스터의 다음 값은 1000 이 되어 0000 으로 고정되는 것을 방지한다.

<48> 마찬가지로, 레지스터(110-140)의 값이 1111 이고 랜덤신호도 1이 되는 경우에, 고정값방지회로(300)를 추가하지 않으면 궤환회로(200)의 출력값이 0이므로 이 궤환회로 출력값과 랜덤신호를 합한 쉬프트 레지스터(100)의 입력값은 1이 되어 쉬프트 레지스터의 값은 계속해서 1111 을 유지하게 된다. 반면, 고정값방지회로(300)를 추가하게 되면 레지스터(110-140)의 값 및 랜덤신호를 반전한 후 논리 곱(320)하는 출력은 1이 되므로, 논리합(330)의 출력인 고정값 방지회로(300)의 출력도 1이 되어, 고정값 방지회로의 출력 값, 랜덤신호, 그리고 궤환회로의 출력값을 합한 회로(500)의 출력인 쉬프트 레지스터(100)의 입력값은 0이 된다. 결국 클럭에 의해 생성되는 쉬프트 레지스터(100)의 다음 값은 0111 이 되어 1111 로 고정되는 것을 방지한다. 정리하여 설명하면, 고정값 방지회로(300)는 쉬프트 레지스터(100)의 모든 값 및 랜덤신호가 동일한 값을 가지는 경우에만 1을 출력시켜, 이 경우의 쉬프트 레지스터 입력값을 반전시키는 효과를 유발한다.

<49> 이해를 돕기 위해 4비트의 경우를 예를 들었으나, 본 발명의 난수 발생 장치는 특정 비트에 국한되지 않고 기존의 선형궤환 쉬프트레지스터를 구성할 수 있는 어떠한 비트 길이에도 적용된다.

<50> 도 4는 독립적인 소스를 가지는 두개의 클럭을 생성한 후 클럭 1은 플립플롭(400A)의 클럭단자에 인가하고 나머지 클럭2는 플립플롭(400A)의 데이터 단자에 인가하여 하나의 클럭이 또 다른 클럭을 샘플링함으로써 랜덤한 신호를 생성하는 회로를 나타낸 것이다. 모든 클럭은 클럭의 값이 변화하는 시점이 매 클럭마다 일정치 않은 지트 성분을 가지고 있으며, 이 지트는 온도 등의 물리적 현상에 의해 발생하며 가운시안 분포를 가지는 랜덤성을 가진다. 만약 샘플링하는 구간이 클럭의 지트가 발생하는 구간이 되면 생성되는 신호는 랜덤한 신호가 된다. 지트의 시간 폭이 작기 때문에 랜덤한 신호가 발생할 확률은 작지만 이 신호를 본 특허에서 제시하는 선형궤환 쉬프트 레지스터에 입력하는 경우는 랜덤신호가 발생할 때마다 레지스터의 값이 예측할 수 없는 값으로 바뀌므로, 아날로그회로를 사용하지 않고 클럭에서 발생하는 랜덤성만을 이용하더라도 물리적 난수를 생성할 수 있다.

<51> 도 5는 독립적인 소스를 가지는 두개의 클럭을 이용하여 랜덤신호를 생성하는 또 다른 예이다. 클럭1을 플립플롭의 클럭 단지에 입력하는 경우, 플립플롭 1(410)에는 그대로 입력하고, 플립플롭 2(420)에는 반전하여 입력함으로써 플립플롭 1(410)은 클럭의 라이징 에지에서 클럭 2의 값을 샘플링하고, 플립플롭 2(420)는 클럭의 폴링 에지에서 클럭 2의 값을 샘플링하게 된다. 이 두개의 플립플롭의 출력값을 합(430)하여 랜덤신호를 생성한다.

<52> 도 4가 클럭의 라이징 에지에서 다른 클럭을 샘플링하는 경우인 반면, 도 5는 클럭의 라이징 및 폴링 에지 모두에서 다른 클럭을 샘플링함으로써 클럭의 지트를 샘플링할 확률은 두배로 증가하게 된다.

<53> 도 6은 본 발명에 따른 디지털 로직을 이용한 난수 발생 방법의 일 실시예의 흐름도이다.

<54> 먼저, 쉬프트 레지스터 내부에 저장된 비트 값들을 순차적으로 이동시키고(600), 쉬프트 레지스터에 저장된 비트 값들을 소정 논리연산하여 궤환신호를 생성한다(610).

<55> 여기서 쉬프트 레지스터의 동작 및 궤환신호를 생성방법은 종래의 선형 궤환 쉬프트 레지스터의 방식을 따르게 되지만, 새로운 형태의 쉬프트 레지스터의 입력신호를 생성하고, 쉬프트 레지스터의 고정값을 방지하고, 랜덤신호를 생성하며, 고정 방지값, 랜덤신호 및 궤환신호를 합하여 쉬프트 레지스터에 입력하는 단계를 추가함으로써 전혀 다른 동작 특성을 가지는 난수 발생 방법을 만들 수 있다.

<56> 이어서, 쉬프트 레지스터로 입력되는 외부 신호를 생성한다(630). 이때, 생성된 외부신호의 논리값이 쉬프트 레지스터에 저장된 비트 값과 모두와 동일한 지의 여부에 따라 다음의 두 가지 과정을 각각 수행한다.

<57> 외부신호의 논리값이 쉬프트 레지스터에 저장된 비트 값과 모두와 동일하지 않은 경우, 외부신호와 궤환신호만을 논리연산하여 쉬프트 레지스터로 출력한다(630).

<58> 하지만, 외부신호의 논리값이 쉬프트 레지스터에 저장된 비트 값과 모두와 동일한 경우는 궤환신호, 외부 신호에 쉬프트 레지스터의 비트 값이 고정되지 않도록 하기 위해 생성되는 고정 방지값을 더 논리연산하여 쉬프트 레지스터로 출력한다(640). 본 방법의 보다 상세한 설명은 본 방법의 다른 태양인 장치의 설명을 통해 이미 설명되었으므로 생략한다.

【발명의 효과】

<59> 이 상으로 설명한 바와 같이, 본 발명은 디지털 로직만을 이용하여, 규칙성을 가지고 있지 않으면서 비트 수에 해당하는 모든 값이 발생할 수 있는 완전 난수를 생성하기 위한 수단을 제공하고 있다.

<60> 또한 본 발명의 난수발생장치는 아날로그 회로를 사용하지 않으므로 공정에 의존하지 않고, 복잡한 알고리즘을 사용하지 않으므로 구현이 용이하며, 디지털 로직의 구성이 작은 면적으로 구현이 가능한 형태이므로 전력의 소모가 작다.

<61> 따라서 IC카드와 같은 저전력, 저면적을 필요로 하는 시스템-온-칩(System-On-Chip)의 난수발생장치로 활용될 수 있음은 물론이고, 본 특허의 난수 발생 장치는 기존의 의사 난수 발생 장치처럼 구현이 용이하므로, 보안을 필요로 하는 모든 종류의 시스템에서 활용될 수 있다.

<62> 본 발명이 비록 본 발명의 바람직한 실시예에 의해 설명되었지만, 본 발명의 범위는 이에 한정되어서는 아니 되고, 청구범위에 의해 뒷받침되는 한 상기 실시예의 변형이나 개량에도 미쳐야 할 것이다.

【특허청구범위】

【청구항 1】

내부에 저장된 비트 값들을 순차적으로 이동시키는 쉬프트 레지스터;

상기 쉬프트 레지스터에 저장된 비트 값들을 소정 논리연산하여 생성한 궤환신호를 생성하는 궤환회로;

상기 쉬프트 레지스터로 입력되는 외부 신호를 생성하는 외부신호 생성회로; 및

상기 궤환신호 및 외부신호를 소정 논리연산하여 상기 쉬프트 레지스터로 출력하는 입력 논리회로를 포함하는 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 장치.

【청구항 2】

제 1항에 있어서, 상기 쉬프트 레지스터의 비트 값 및 외부 신호의 논리값이 모두 동일한 경우, 상기 입력 논리회로의 출력값이 상기 쉬프트 레지스터의 비트 값과 다른 값이 되도록 하는 값을 상기 입력 논리회로로 출력하는 고정값 방지회로를 더 포함하는 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 장치.

【청구항 3】

제 2항에 있어서, 상기 고정값 방지회로의 출력은 논리값 하이인 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 장치.

【청구항 4】

제 1항에 있어서, 상기 외부 신호 생성회로는 랜덤신호를 생성하는 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 장치.

【청구항 5】

제 4항에 있어서, 상기 랜덤신호는 발생원이 다른 신호를 샘플링함으로써 생성되는 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 장치.

【청구항 6】

제 5항에 있어서, 상기 샘플링은 신호의 라이징 에지 및 폴링 에지에서 모두 수행되는 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 장치.

【청구항 7】

(1) 쉬프트 레지스터 내부에 저장된 비트 값들을 순차적으로 이동시키는 단계;

(2) 상기 쉬프트 레지스터에 저장된 비트 값들을 소정 논리연산하여 궤환신호를 생성하는 단계;

(3) 상기 쉬프트 레지스터로 입력되는 외부 신호를 생성하는 단계; 및

(4) 상기 궤환신호 및 외부신호를 소정 논리연산하여 상기 쉬프트 레지스터로 출력하는 단계를 포함하는 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 방법.

【청구항 8】

제 7항에 있어서, 상기 (4)단계는,

상기 쉬프트 레지스터의 비트 값 및 외부 신호의 논리값이 모두 동일한 경우, 상기 쉬프트 레지스터로의 출력값이 상기 쉬프트 레지스터의 비트 값과 다른 값이 되도록 하는 고정 방지값을 더 논리연산하는 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 방법.

【청구항 9】

제 8항에 있어서, 상기 고정 방지값은 논리값 하이인 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 방법.

【청구항 10】

제 7항에 있어서, 상기 외부 신호는 랜덤신호인 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 방법.

【청구항 11】

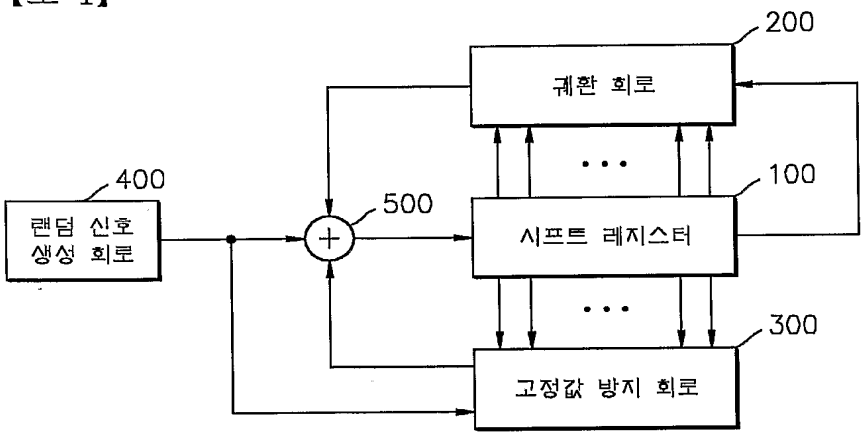
제 10항에 있어서, 상기 랜덤신호는 발생원이 다른 신호를 샘플링함으로써 생성되는 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 방법.

【청구항 12】

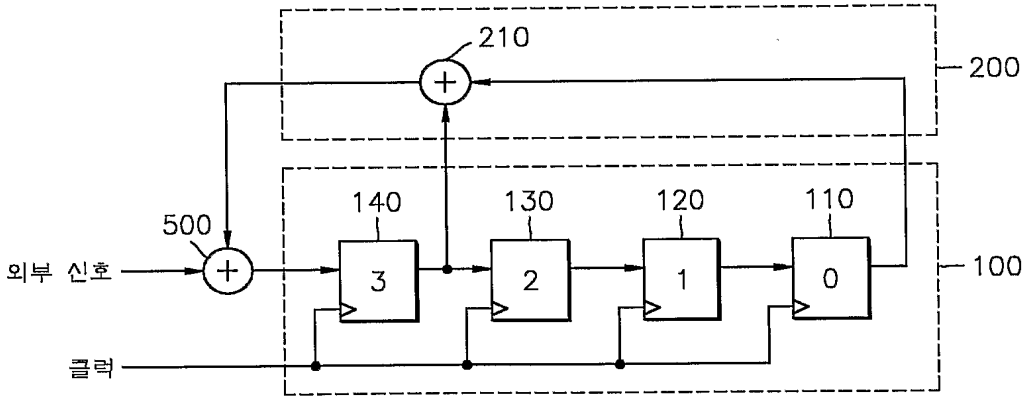
제 11항에 있어서, 상기 샘플링은 신호의 라이징 에지 및 폴링 에지에서 모두 수행되는 것을 특징으로 하는 디지털 로직을 이용한 난수 발생 방법.

【도면】

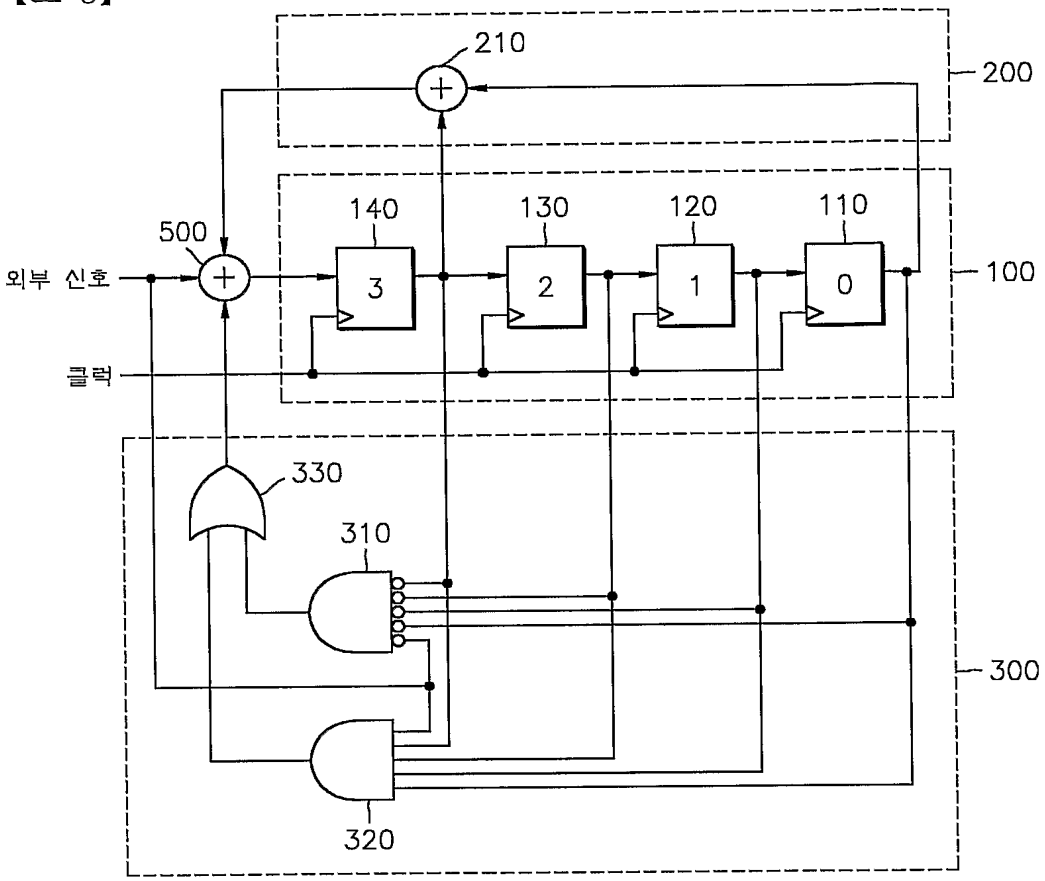
【도 1】


200
궤환 회로
100
시프트 레지스터
300
고정값 방지 회로
400
랜덤 신호
생성 회로
500

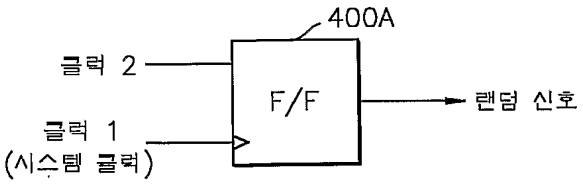
【도 2】


210
200
140
130
120
110
500
외부 신호
3
2
1
0
100
클럭

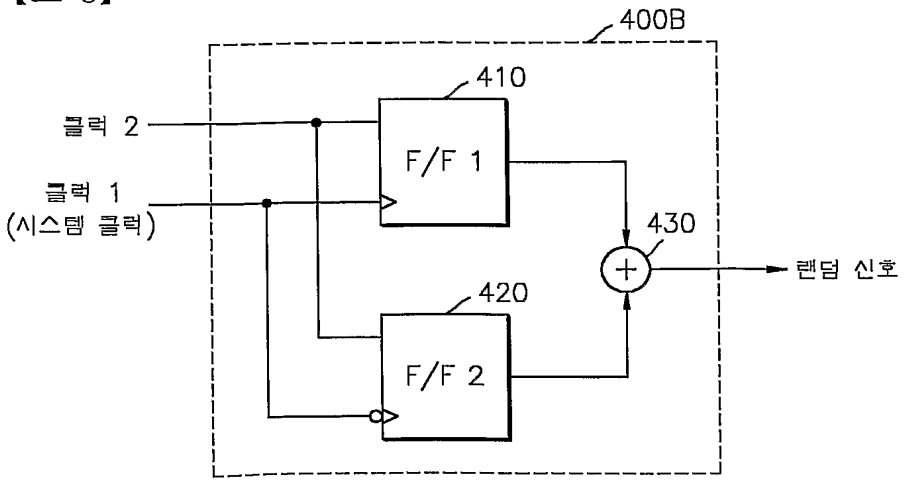
【도 3】


210
200
140
130
120
110
500
외부 신호
3
2
1
0
100
클럭
330
310
300
320

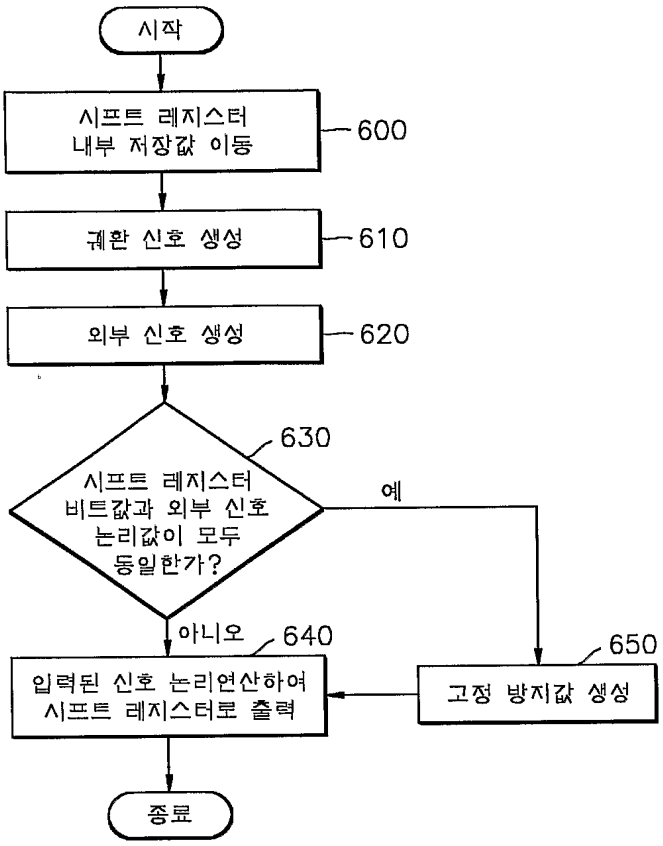
【도 4】


400A
클럭 2
F/F
랜덤 신호
클럭 1
(시스템 클럭)

【도 5】


400B
410
클럭 2
F/F 1
클럭 1
(시스템 클럭)
430
랜덤 신호
420
F/F 2

【도 6】


시작
시프트 레지스터 내부 저장값 이동
600
궤환 신호 생성
610
외부 신호 생성
620
630
시프트 레지스터 비트값과 외부 신호 논리값이 모두 동일한가?
예
아니오
640
650
입력된 신호 논리연산하여 시프트 레지스터로 출력
고정 방지값 생성
종료